Comparative Remediation Testing Report

A test commissioned by Enigma Software Group and performed by AV-Test GmbH
Date of the report: May 10th, 2017, last update May 24th, 2017

Executive Summary

In March 2017, AV-Test performed a comparison test of Enigma Software Group's SpyHunter remediation capabilities. The test has been run on a clean Windows 7 (SP1, 64-bit). The same disk image was used on several identical PCs.

The malware test corpus for the remediation test consisted of 21 samples and was divided into two parts. Test Part 1: First, the image was infected with one of the malware samples. The next step was trying to install the security product, scanning the PC and removing any threats that have been found. Test Part 2: In the second, part the AV was disabled to infect the system. Then, the AV was enabled again and to ensure that all components of the AV are enabled correctly a reboot was performed. The next step was trying to remediate the system and performing a system scan additionally.

Test Part 1: SpyHunter scored almost perfect with 98% and cleaned all active components of the malware only in one case a created task of the malware was left on the system. The next three products, Emsisoft Anti-Malware, Malwarebytes Free and Malwarebytes Premium scored also well with 92-93% here. Spybot Search & Destroy and IOBit Malware Fighter follow with clear distance and a very poor result of only 40% and 10%.

Test Part 2: In this part, we have the same sequence as in Test Part 1. SpyHunter scored very good 97% and are able to clean all active parts of the malware and left only a start entry in the registry and the created tasks on the system. Emsisoft Anti-Malware, Malwarebytes Free and Malwarebytes Premium also scored with a good result of 92-93% and Spybot and IObit are far away with 40% and 10%.

Overview

With the increasing number of threats that is being released and spread through the Internet these days, the danger of getting infected is increasing as well. A few years back there were new viruses released every few days. This has grown to several thousand new threats per hour.

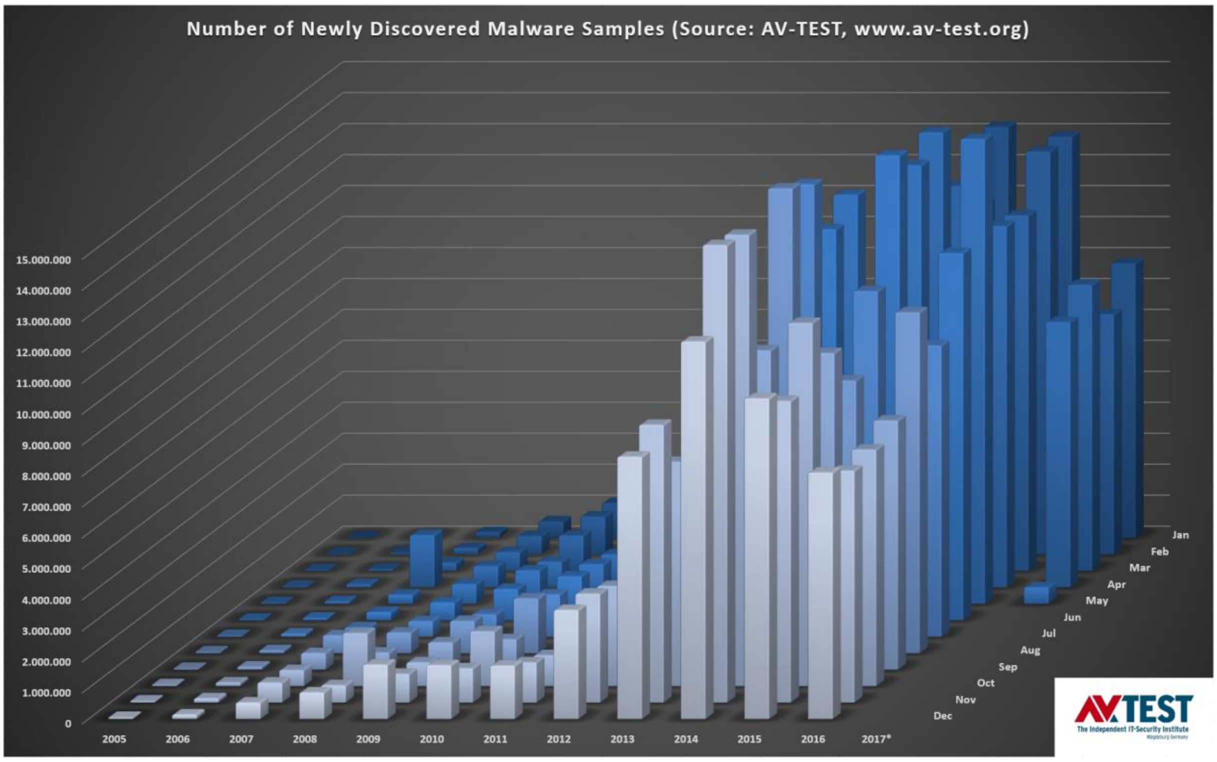

Figure 1: New samples added per year

In the year 2000, AV-Test received more than 170,000 new samples, and in 2013, the number of new samples grew to over 80,000,000 new samples. The numbers continued to grow in the year 2016. The growth of these numbers is displayed in Figure 1. AV-TEST has currently over 630 million malware samples in its database.

The volume of new samples that have to be processed by anti-malware vendors in order to protect their customers can create problems. It is not always possible to successfully protect a PC in time. Even if up-to-date anti-malware software is installed, it is possible that a PC can get infected because signatures are provided only every few hours, which sometimes may be too late. Infections create financial loss, either because sensitive data is stolen or because the PC cannot be used for productive work anymore until the malware has completely removed from the system.

Therefore, remediation techniques become more important to get an infected PC up and running again. In that process, it is imperative that the cleaning process is reliable in two ways:

1. The malware and all of its components have to be removed and any malicious system changes have to be reverted.
2. No clean applications or the system itself must be harmed by the cleaning process.

Products Tested

The testing occurred in March. AV-TEST used the latest releases available at the time of the test of:

- Enigma Software Group's SpyHunter
- Emsisoft Anti-Malware
- IOBit Malware Fighter
- Malwarebytes Free
- Malwarebytes Premium
- Safer Networking Spybot - Search & Destroy

Methodology and Scoring

Platform

All tests have been performed on identical PCs equipped with the following hardware:

- Intel Xeon Quad-Core X3360 CPU
- 4 GB Ram
- 500 GB HDD (Western Digital)
- Intel Pro/1000 PL (Gigabit Ethernet) NIC

The operating system was Windows 7 (SP1, 64-bit) with only those hotfixes that were part of this version as well as all patches that were available on January 3rd 2017

Testing methodology

The remediation test has been performed according to the methodology explained below.

1. **Clean system for each sample**. The test systems should be restored to a clean state before being exposed to each malware sample.
2. **Physical Machines**. The test systems used should be actual physical machines. No Virtual Machines should be used.
3. **Internet Access**. The machines had access to the Internet at all times, in order to use in-the-cloud queries if necessary.
4. **Product Configuration**. All products and their accompanying remediation tools or bootable recovery tools were run with their default, out-of-the-box configuration.
5. **Infect test machine**. Infect native machine with one threat, reboot and make sure that threat is fully running.
6. **Sample Families and Payloads**. No two samples should be from the same family or have the same payloads.
7. **Remediate using all available product capabilities**.
    a. Try to install security product in default settings. Follow complete product instructions for removal.
    b. If a. doesn't work, try ***standalone fixtool/rescue tool*** solution (if available).
    c. If b. doesn't work, boot standalone ***boot solution*** (if available) and use it to remediate.
8. **Validate removal**. Manually inspect PC to validate proper removal and artifact presence.

9. **Score removal performance**. Score the effectiveness of the tool and the security solution as a whole using the agreed upon scoring system.
10. **Overly Aggressive Remediation**. The test should also measure how aggressive a product remediates. For example some products will completely remove the hosts file or remove an entire directory when it is not necessary to do so for successful remediation. This type of behavior should count against the product.

Efficacy Rating

For each sample tested, apply points according to the following schedule:

a. Malware completely removed (3)
b. Detected and removed, only inactive traces remains (2)
c. Something detected and partly removed, but malware traces are still active (1)
d. Not detected, nothing remediated (0)

The scoring should not take into consideration which of the available techniques were needed to remove the malware. All techniques, however, should be applied. When a product cleans out the entries in the hosts file that relate to that very product and leave the machine uninfected and the product functional and updateable, it should be given full credit for remediation even if entries for other security vendors remain in the hosts file.

Samples

The set contained 21 malicious files that were able to infect Windows 7 (SP1, 64-bit).

Test Results

SpyHunter scored best in this test and achieved 123 out of 126 possible points. In second place are both Malwarebytes Editions with a good result of 118 points achieved. Right behind it, comes Emsisoft Anti-Malware with also good received 116 points. Spybot Search & Destroy reached only 50 points in total, followed by IOBit Malware Fighter with a very poor result of only 12 out of 126 points.

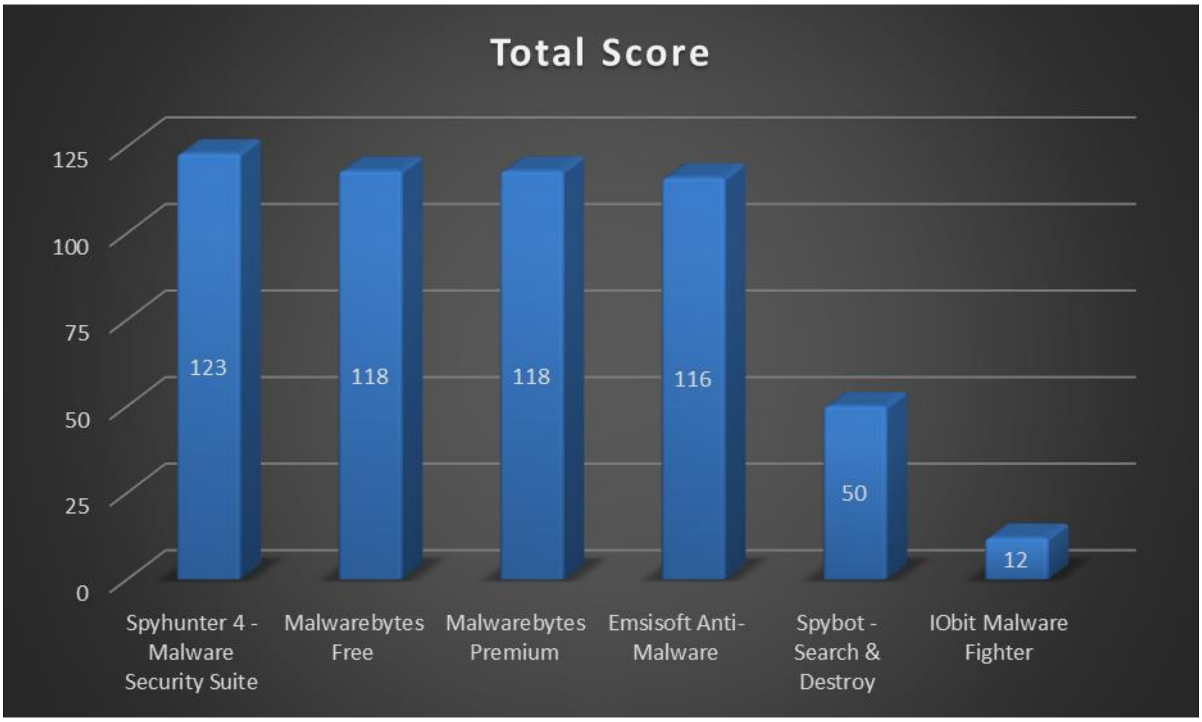

Figure 2: Remediation Total Score – Part 1.1 +1.2

The results of the Test Parts 1 & 2 are nearly identical and shown in the Figure 3 and 4. The maximum achievable points are 63 for Test Part 1 and 2.

SpyHunter achieved very good 62 points in Test Part 1 and 61 in Test Part 2. In both test parts SpyHunter left a task on the system and additionally a registry entry in part 2.

Both Malwarebytes versions received good 59 points but one test case could not be cleaned and active parts of the malware remain on the system. On the third place is Emsisoft Anti-Malware with 58 points. Anti-Malware cleaned all active components of the 21 tested samples and left a task and registry entries on the system.

Spybot solution Search & Destroy received only 25 points in Test Part 1 and 25 in Part 2 and more than half of the tested samples were not cleaned.

The worst result reached IOBit with only 6 points in each Test Part. IOBit was not able to clean 18 of 21 tested samples.

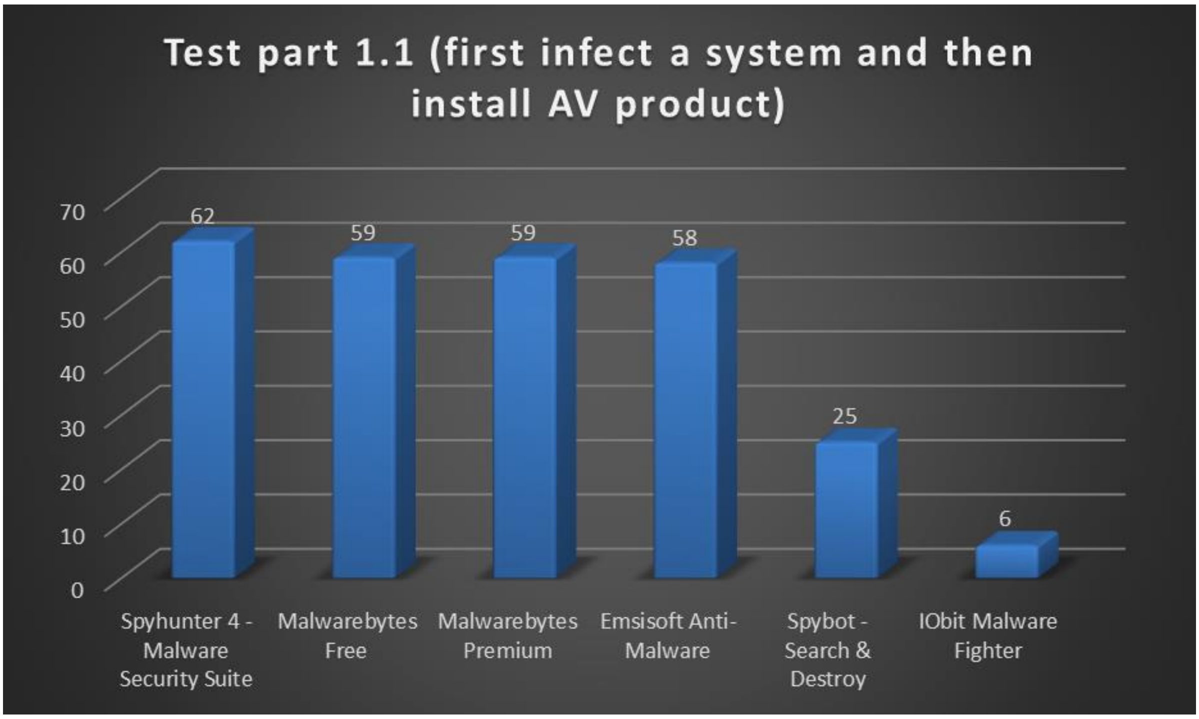

Figure 3: Remediation Score – Test Part 1.1

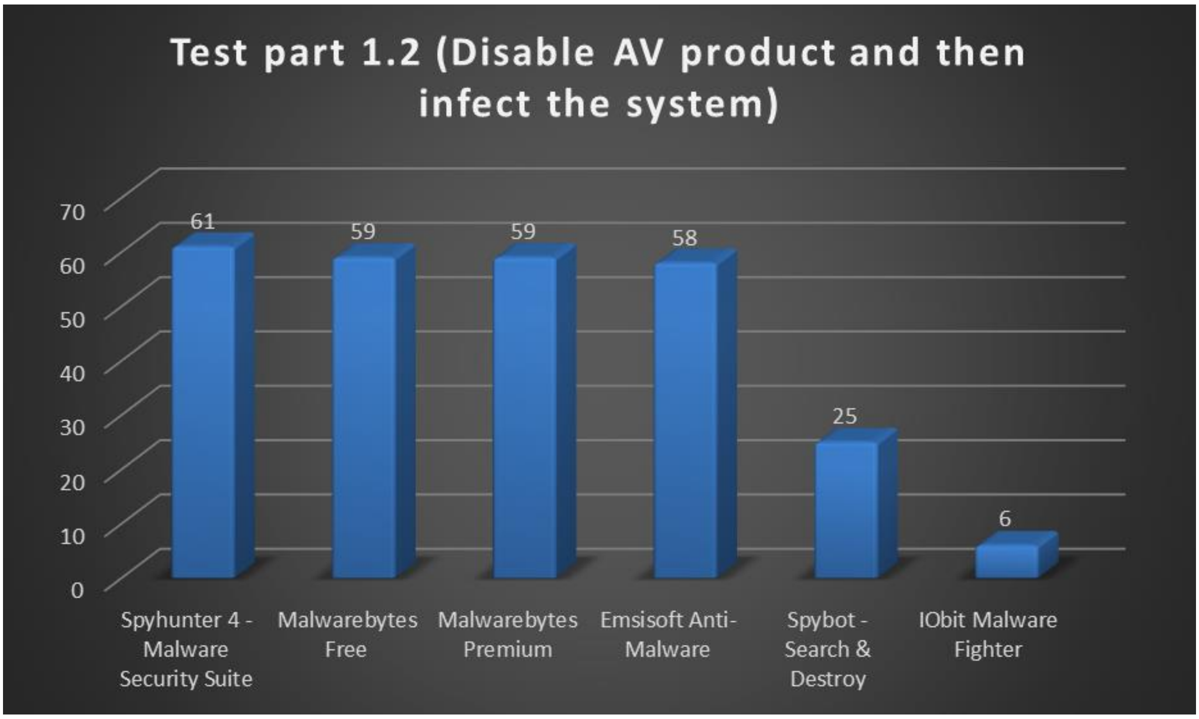

Figure 4: Remediation Score – Test Part 1.2

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Emsisoft	Anti-Malware	2017.2.1.7260	4.0.1.856/20170324
Enigma Software Group	SpyHunter 4	4.25.6.4782	2017.03.23v01
IOBit	Malware Fighter	4.5.0.3457	1634
Malwarebytes	Malwarebytes Free	3.0.6.1469	n/a
Malwarebytes	Malwarebytes Premium	3.0.6.1469	n/a
Safer Networking	Spybot - Search & Destroy	1.6.2.46	n/a

List of used malware samples (Remediation Test)

(SHA256)
* 0x0101d4a72a3685aaf8a7baa4408223914ba7f1c8d193628fabbe98cd377536cd
* 0x01168762ca9a57ffe5b69371b85d7d60339a3a95091554e87750715fc146313d
* 0x0bf7ab1fd378c78ea8206c84dfa780c472d84c5357238d78df369881f762ad99
* 0x246082bd340133a0b634ef874a20f9823336fc3e65baddaddc57c3af5588a35a
* 0x369fab397bbc2ca10601c3ca89f77b24eecf485b080f07d820daf8a6487554a2
* 0x3b56fcb59462dac54bee27b85bc8e29af286d0349909aa9a313868e8be5c96bd
* 0x453442bc8fd9e0fec64febb1c7c81cc1daecc151faa0aa30041b25296b906423
* 0x454ecf8d9846abae025fa57f097fa6bc11b3ac7bd68b9a1c2eb55bc6861b3d4c
* 0x4b91c4e2f69697a888b56147f69d4c96ca13095a2aaf640a48e68994c7228565
* 0x4da0d3e569ceeced62b7128ed35c55cfb48236be628ba64411f066a9a38a5aff
* 0x4e59b6263b5b3a5ce4ea5054dc48cca37945ca930ad1a5aa300029539d8042a3
* 0x6a9936983ee1bc49d5fff7e2ae6435462667c7f62547a710297b8f9c86a36873
* 0x7021df3d38a24a1de948ef5c820b60d8e61c95ed3409c255680eba79e4221123
* 0x7a1e9db7fe1bc6341b1e1a002c19ca6f32224aa0c4eb6582d984d66bb44f339e
* 0x8f995f37b1aee61018742c35ab410820b02982fe2ac0b9a2554d02909f2590a2
* 0x9643447291f6e468611c8acb6e58f8e3b3c40a3394e4f7d5c20489a9af0e0750
* 0xc0d110efbd58448c8fed7e249a3e5503185cd3f2fc4a13339874646256877f9e
* 0xda3458870afb6487c435129bd1ac4c8b994c2133d3790ca505949cc2644293bf
* 0xee7e9a572dd14739aaf6cc16f1d52e66b62347f1902a2c93a9145ab9c0f29d83
* 0xf6c186da15892176e8f8cd31e9dd637024a4e4e08510315011d6d735a32f2c93

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web http://www.av-test.org